Z/OS TOP TEN CRITICAL ASSESSMENT FINDINGS

Presented by Brian Marshall,

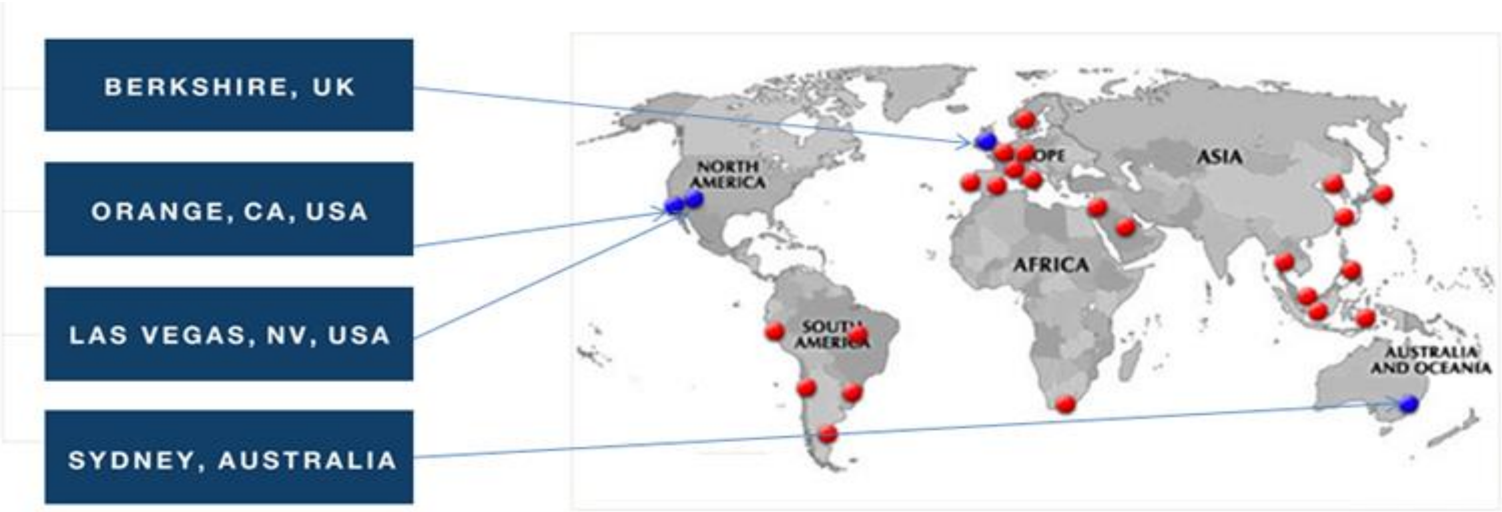
Vice President, Research and Development

Vanguard Integrity Professionals

About Vanguard

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Founded:	1986
Business:	Cybersecurity Experts for Large Enterprises Software, Professional Services, and Training
Customers:	1,000+ Worldwide



Over 15 distributors/resellers serving 50+ countries worldwide

IBM Server Proven

Business Partner IBM

The Mainframe

ComputerWeekly.com

Mainframe at 50: Why the mainframe keeps on going

For the past 50 years, the mainframe has been the technological workhorse enab

In fact, 80% of the world's corporate data is still managed by mainframes.

In a video interview with Computer Weekly's Cliff Saran, IBM Hursley lab director
in computing paradigms and application systems, such as the move to the web and mobile technology.

> " 80% of the world’s corporate data is still managed by mainframes."

"The platform is continually reinventing itself to remain relevant for cloud and mobile computing and to be able to run the most popular application server packages," he said.
Yet while it appears to be middle-aged technology, in terms of reach it seems the mainframe touches almost everything in modern life, according to Lamb.

“If you are using a mobile application today that runs a trans
another, there is a four in five chance that there is a mainfra

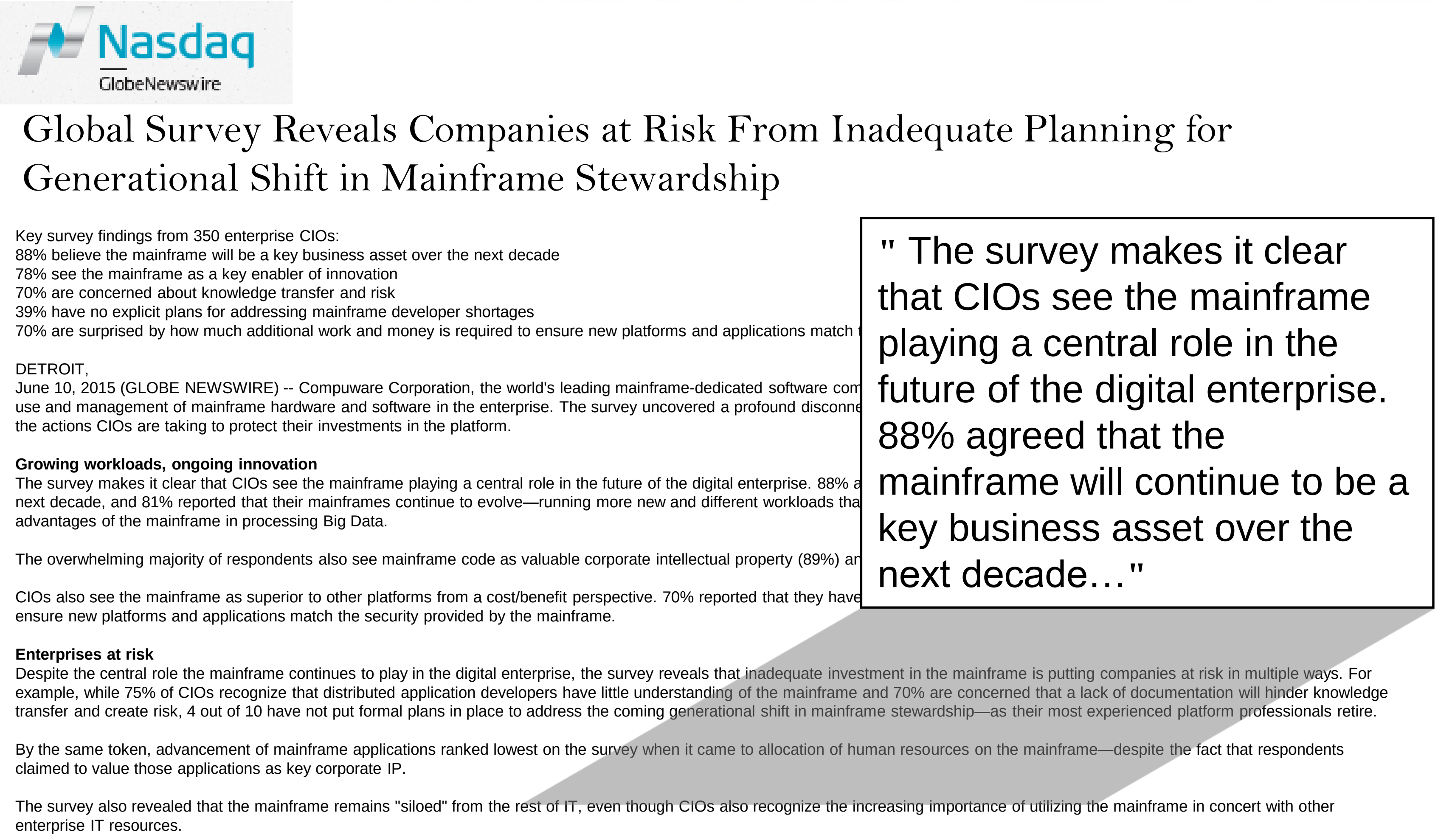
And the amount of processing run on the mainframe dwarfs
likes and 60,000 Google searches. But the CICs application
per second – that's 100 billion transactions a day," he said.

IBM will be formally celebrating the 50th anniversary of the S

> "If you are using a mobile application today that runs a transaction to check your bank balance or transfer money from one account to another, there is a four in five chance that there is a mainframe behind that transaction."

Source: Computer Weekly; Interview with Rob Lamb, IBM Hursley lab director, March 24, 2014

Mainframe Survey of 350 CIO's



Nasdaq GlobeNewswire

Global Survey Reveals Companies at Risk From Inadequate Planning for Generational Shift in Mainframe Stewardship

Key survey findings from 350 enterprise CIOs:
88% believe the mainframe will be a key business asset over the next decade
78% see the mainframe as a key enabler of innovation
70% are concerned about knowledge transfer and risk
39% have no explicit plans for addressing mainframe developer shortages
70% are surprised by how much additional work and money is required to ensure new platforms and applications match t

DETROIT,
June 10, 2015 (GLOBE NEWSWIRE) -- Compuware Corporation, the world's leading mainframe-dedicated software com
use and management of mainframe hardware and software in the enterprise. The survey uncovered a profound disconne
the actions CIOs are taking to protect their investments in the platform.

Growing workloads, ongoing innovation
The survey makes it clear that CIOs see the mainframe playing a central role in the future of the digital enterprise. 88% a
next decade, and 81% reported that their mainframes continue to evolve—running more new and different workloads tha
advantages of the mainframe in processing Big Data.

The overwhelming majority of respondents also see mainframe code as valuable corporate intellectual property (89%) an

CIOs also see the mainframe as superior to other platforms from a cost/benefit perspective. 70% reported that they have
ensure new platforms and applications match the security provided by the mainframe.

Enterprises at risk
Despite the central role the mainframe continues to play in the digital enterprise, the survey reveals that inadequate investment in the mainframe is putting companies at risk in multiple ways. For example, while 75% of CIOs recognize that distributed application developers have little understanding of the mainframe and 70% are concerned that a lack of documentation will hinder knowledge transfer and create risk, 4 out of 10 have not put formal plans in place to address the coming generational shift in mainframe stewardship—as their most experienced platform professionals retire.

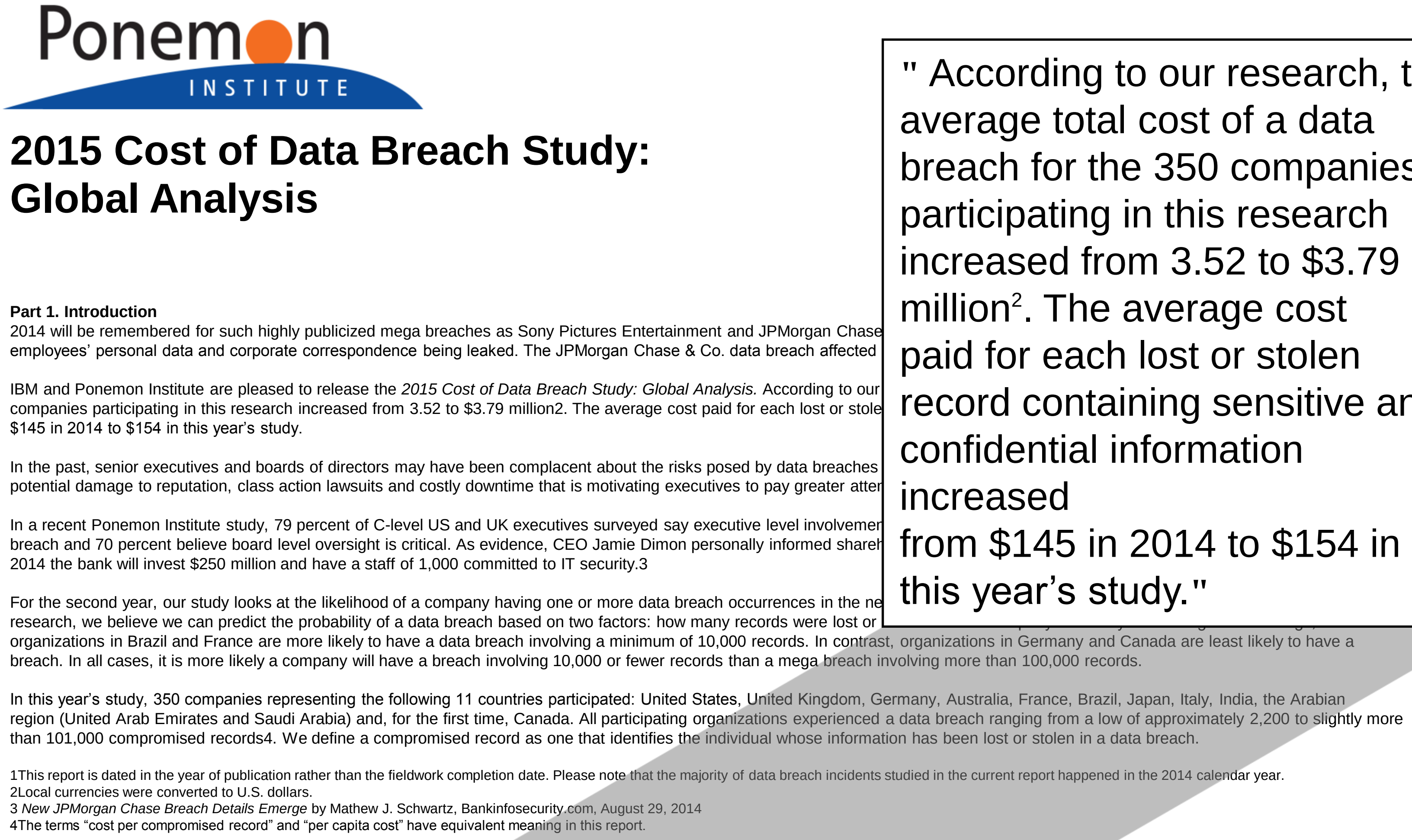
By the same token, advancement of mainframe applications ranked lowest on the survey when it came to allocation of human resources on the mainframe—despite the fact that respondents claimed to value those applications as key corporate IP.

The survey also revealed that the mainframe remains "siloed" from the rest of IT, even though CIOs also recognize the increasing importance of utilizing the mainframe in concert with other enterprise IT resources.

" The survey makes it clear that CIOs see the mainframe playing a central role in the future of the digital enterprise. 88% agreed that the mainframe will continue to be a key business asset over the next decade…"

Source: Nasdaq GlobeNewswire, Compuware Corporation, June 10, 2015

Cost of a Data Breach



2015 Cost of Data Breach Study: Global Analysis

Part 1. Introduction
2014 will be remembered for such highly publicized mega breaches as Sony Pictures Entertainment and JPMorgan Chase
employees' personal data and corporate correspondence being leaked. The JPMorgan Chase & Co. data breach affected

IBM and Ponemon Institute are pleased to release the *2015 Cost of Data Breach Study: Global Analysis.* According to our
companies participating in this research increased from 3.52 to $3.79 million2. The average cost paid for each lost or stole
$145 in 2014 to $154 in this year's study.

In the past, senior executives and boards of directors may have been complacent about the risks posed by data breaches
potential damage to reputation, class action lawsuits and costly downtime that is motivating executives to pay greater atter

In a recent Ponemon Institute study, 79 percent of C-level US and UK executives surveyed say executive level involvemer
breach and 70 percent believe board level oversight is critical. As evidence, CEO Jamie Dimon personally informed shareh
2014 the bank will invest $250 million and have a staff of 1,000 committed to IT security.3

For the second year, our study looks at the likelihood of a company having one or more data breach occurrences in the ne
research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or
organizations in Brazil and France are more likely to have a data breach involving a minimum of 10,000 records. In contrast, organizations in Germany and Canada are least likely to have a
breach. In all cases, it is more likely a company will have a breach involving 10,000 or fewer records than a mega breach involving more than 100,000 records.

In this year's study, 350 companies representing the following 11 countries participated: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, the Arabian
region (United Arab Emirates and Saudi Arabia) and, for the first time, Canada. All participating organizations experienced a data breach ranging from a low of approximately 2,200 to slightly more
than 101,000 compromised records4. We define a compromised record as one that identifies the individual whose information has been lost or stolen in a data breach.

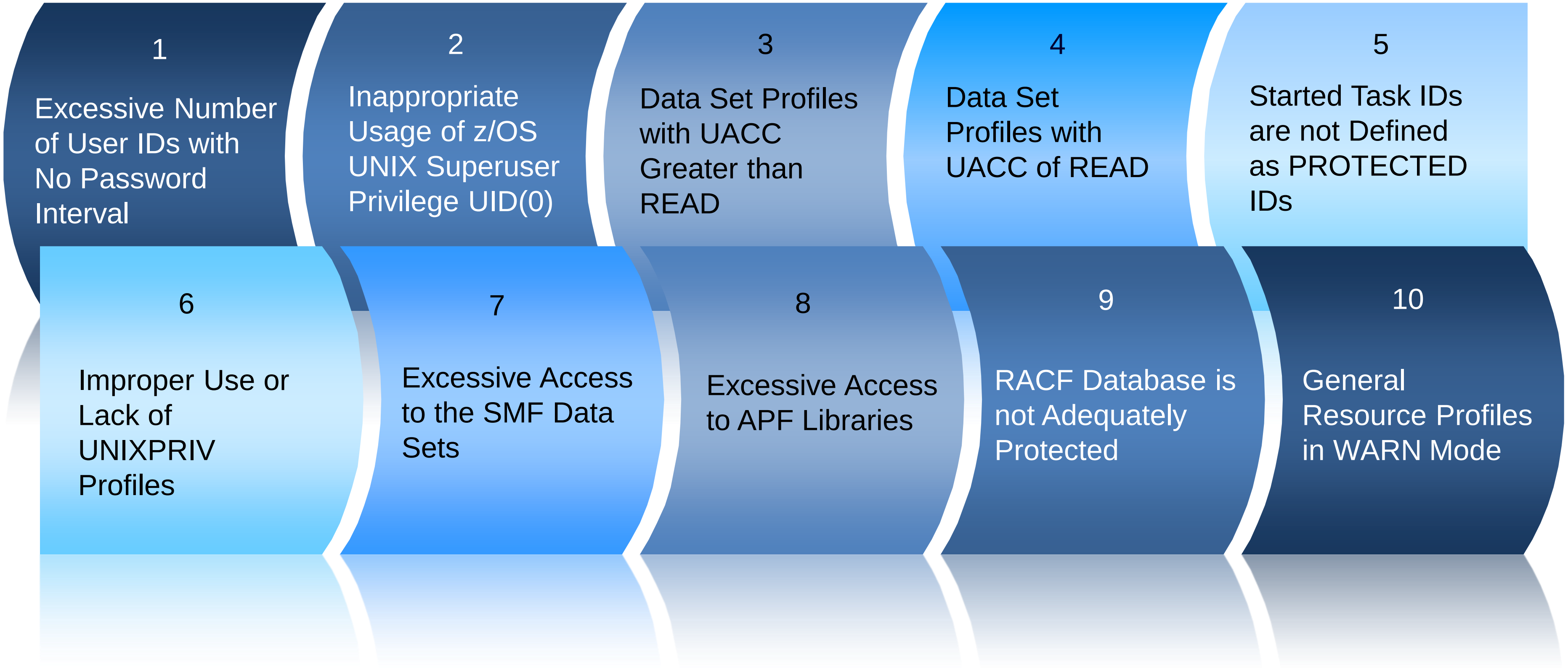
1This report is dated in the year of publication rather than the fieldwork completion date. Please note that the majority of data breach incidents studied in the current report happened in the 2014 calendar year.
2Local currencies were converted to U.S. dollars.
3 *New JPMorgan Chase Breach Details Emerge* by Mathew J. Schwartz, Bankinfosecurity.com, August 29, 2014
4The terms "cost per compromised record" and "per capita cost" have equivalent meaning in this report.

" According to our research, the average total cost of a data breach for the 350 companies participating in this research increased from 3.52 to $3.79 million[2]. The average cost paid for each lost or stolen record containing sensitive and confidential information increased
from $145 in 2014 to $154 in this year's study."

Source: Ponemon Institute® Research Report, May, 2015

Vulnerability Assessment Findings

Scope: Vanguard Top 10 z/OS Risks Identified in Client Security Assessments



1 Excessive Number of User IDs with No Password Interval

2 Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

3 Data Set Profiles with UACC Greater than READ

4 Data Set Profiles with UACC of READ

5 Started Task IDs are not Defined as PROTECTED IDs

6 Improper Use or Lack of UNIXPRIV Profiles

7 Excessive Access to the SMF Data Sets

8 Excessive Access to APF Libraries

9 RACF Database is not Adequately Protected

10 General Resource Profiles in WARN Mode

Note: Data collected from hundreds of security assessments performed by Vanguard Integrity Professionals.

“Top Ten” Assessment Finding #1

Finding

Excessive Number of User IDs with No Password Interval

Explanation

User IDs with no password Interval are not required to change their passwords.

Risk

Since passwords do not need to be changed periodically, people who knew a password for an ID could still access that ID even if they are no longer authorized users.

Recommended Best Practice and Remediation

Review each of the personal user profiles to determine why they require NOINTERVAL. Their passwords should adhere to the company policy regarding password changes. If the user ID is being used for started tasks or surrogate, it should be reviewed and changed to PROTECTED.

“Top Ten” Assessment Finding #2

Finding

Inappropriate Usage of z/OS UNIX Superuser Privilege UID(0)

Explanation

User IDs with z/OS UNIX superuser authority, UID(0), have full access to all UNIX directories and files and full authority to administer z/OS UNIX.

Risk

Since the UNIX environment is the z/OS portal for critical applications such as file transfers, Web applications, and TCPIP connectivity to the network in general, the ability of these superusers to accidentally or maliciously affect these operations is a serious threat. No personal user IDs should be defined with an OMVS segment specifying UID(0).

Recommended Best Practice and Remediation

The assignment of UID(0) authority should be minimized by managing superuser privileges by granting access to one or more of the ‘BPX.qualifier’ profiles in the FACILITY class and access to one or more profiles in the UNIXPRIV class..

“Top Ten” Assessment Finding #3

Finding

Data Set Profiles with UACC Greater than READ

Explanation

The UACC value for a dataset profile defines the default level of access to which any user whose user ID or a group to which it has been connected does not appear in the access list.

Risk

Data sets that are protected by a RACF profile with a UACC greater than READ allow most users with system access to read or modify these data sets. In addition, users may be able to delete any data set covered by the dataset profiles that have a UACC of ALTER.

Recommended Best Practice and Remediation

Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with greater than READ access.

“Top Ten” Assessment Finding #4

Finding

Data Set Profiles with UACC of READ

Explanation

The UACC value for a dataset profile defines the default level of access to which any user whose user ID or a group to which it has been connected does not appear in the access list.

Risk

Data sets that are protected by a RACF profile with a UACC of READ will allow most users with system access to read or copy sensitive and critical data residing in these data sets.

Recommended Best Practice and Remediation

Review each of these profiles and determine whether the UACC is appropriate. For those profiles where the UACC is excessive, you will have to determine who really needs access before changing the UACC. To find out who is accessing these data sets, review SMF data to determine who is accessing the data sets with READ access.

“Top Ten” Assessment Finding #5

Finding

Started Task IDs are not Defined as PROTECTED IDs

Explanation

User IDs associated with started tasks should be defined as PROTECTED which will exempt them from revocation due to inactivity or excessive invalid password attempts, as well as being used to sign on to an application.

Risk

RACF will allow the user ID to be used for the started task even if it has become revoked, but some started tasks may either submit jobs to the internal reader that will fail or may issue a RACROUTE REQUEST=VERIFY macro for the user ID that will also fail.

Recommended Best Practice and Remediation

Review all started task user IDs that are not protected. Determine if the user IDs are used for any other function that might require a password. Define the started task user IDs as PROTECTED for those tasks that do not require a password.

“Top Ten” Assessment Finding #6

Finding

Improper Use or Lack of UNIXPRIV Profiles

Explanation

The UNIXPRIV class resource rules are designed to give a limited subset of the superuser UID (0) capability. When implemented properly, UNIXPRIV profiles can significantly reduce the unnecessary requests for assignment of UID (0) to user IDs.

Risk

Without the UNIXPRIV profiles defined, administrator IDs would require superuser ability through the assigned UID (0). The ability of these superusers to accidentally or maliciously affect the operation of your z/OS UNIX system is a serious threat.

Recommended Best Practice and Remediation

Review the users’ activity that are currently defined as SUPERUSERs to determine if granular profiles may be defined in the UNIXPRIV class that will authorize their activity. Refine the access list and define more granular profiles based upon the superuser functions that the users with UID(0) need.

“Top Ten” Assessment Finding #7

Finding

Excessive Access to SMF Data Sets

Explanation

SMF data collection is the system activity journaling facility of the z/OS system. With the proper parameter designations, it serves as the basis to ensure individual user accountability.

Risk

The ability to READ SMF data enables someone to identify potential opportunities to breach your security. If UPDATE or higher access is granted, a risk of audit log corruption exists. Access control for the unloaded data is critical to ensure a valid chain of custody.

Recommended Best Practice and Remediation

Ensure that access authority to SMF collection files is limited to only systems programming staff and and/or batch jobs that perform SMF dump processing and ensure the UPDATE and higher accesses are being logged.

“Top Ten” Assessment Finding #8

Finding

Excessive Access to APF Libraries

Explanation

Authorized Program Facility (APF) libraries are an integral part of the z/OS architecture to enable maintenance of the integrity of the z/OS operating system environment. Libraries designated as APF allow programs to execute with the authority of z/OS itself, so the ability to modify these libraries must be strictly controlled.

Risk

UPDATE or higher access to an APF library can allow an individual to create an authorized program which can bypass security controls and execute privileged instructions. UPDATE or higher access should be limited to senior systems support staff.

Recommended Best Practice and Remediation

Review the protection of all APF libraries and remove or change inappropriate access list entries and ensure that all UPDATE activity is logged to SMF.

“Top Ten” Assessment Finding #9

Finding	RACF Database is not Adequately Protected
Explanation	The RACF database contains extremely sensitive security information. No access to the RACF database is required for normal administration activities using either RACF commands or the RACF provided ISPF panels.
Risk	Any user who has read access to the RACF database or any backup copy could make a copy and then use a cracker program to find passwords for user IDs and could obtain a list of user IDs and resources.
Recommended Best Practice and Remediation	Review the protection for the RACF database and any backup copies and remove any access list entries granting access higher than NONE, other than to senior RACF administrators and system staff tasked to run RACF database utilities.

“Top Ten” Assessment Finding #10

Finding	General Resource Profiles in WARN Mode
Explanation	General Resource profiles defined in WARN mode specifies that even if access authority is insufficient, RACF is to issue a warning message and allow access to the resource. RACF also records the access attempt in the SMF record.
Risk	Most all users have full access to any resource that is protected by a profile in WARN mode.
Recommended Best Practice and Remediation	Monitor the SMF data on a daily basis to determine if the accesses to these resources are due to the WARN mode. The reports will indicate the usage of these resources for users who are not specifically defined to the access list. If the accesses are appropriate, grant the user/group the access required. Remove WARN mode from all general resource profiles once analysis is complete.

Top Ten Critical Assessment Findings in Mainframe Environments

The percentage numbers represent the percentages of environments in which Vanguard has found this configuration error in over 200 environments in the last 8 years.

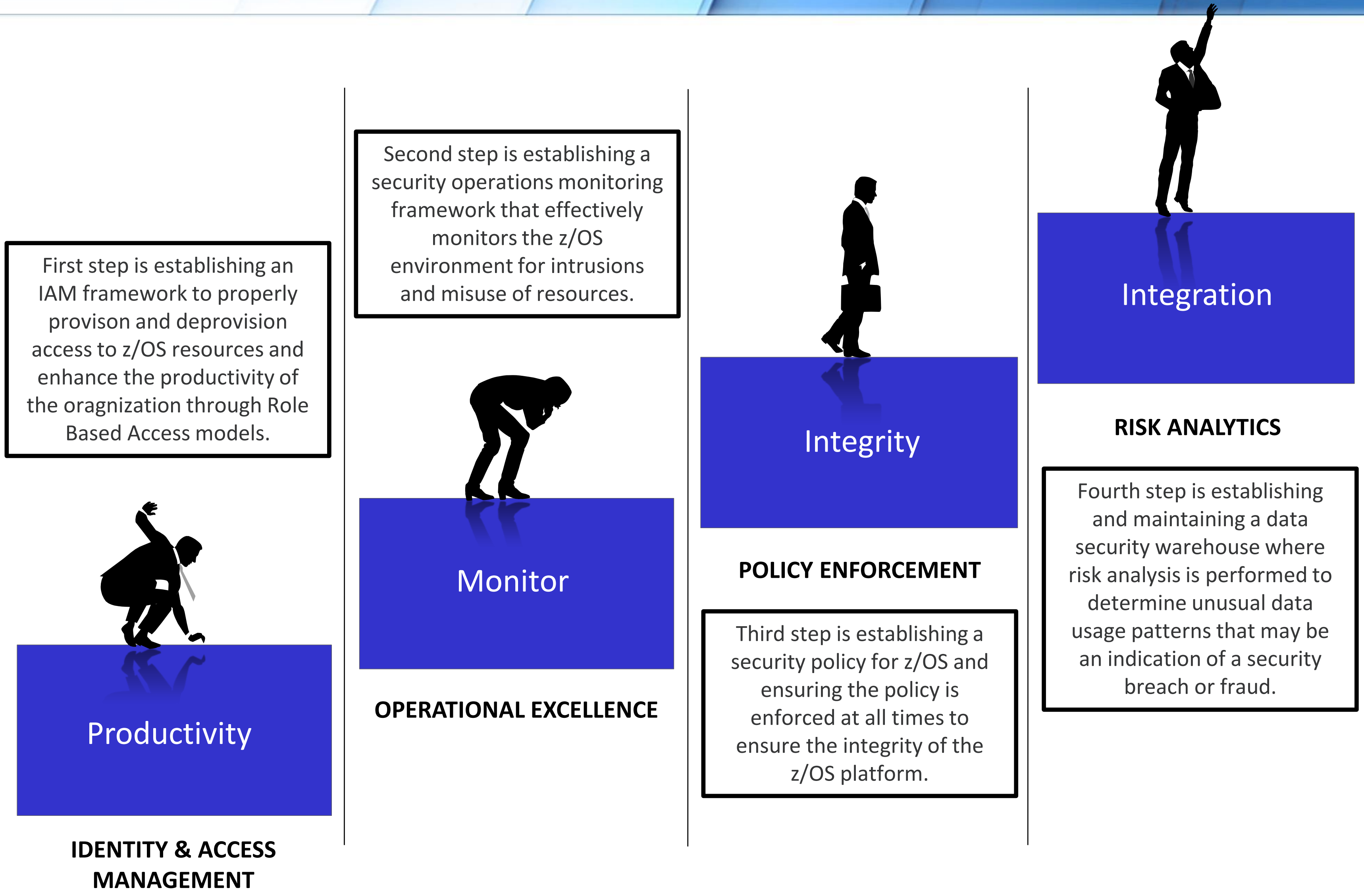
73%	Excessive Number of User ID’s with no Password Interval	SEVERE
60%	Inappropriate Usage of z/OS UNIX Superuser Privilege, UID = 0	SEVERE
53%	Data Set Profiles with UACC Greater than READ	SEVERE
53%	Data Set Profiles with UACC of READ	HIGH
52%	Started Task IDs are not Defined as PROTECTED IDs	HIGH
51%	Improper Use or Lack of UNIXPRIV Profiles	HIGH
44%	Excessive Access to the SMF Data Sets	HIGH
42%	Excessive Access to APF Libraries	SEVERE
40%	RACF Database is not Adequately Protected	SEVERE
39%	General Resource Profiles in WARN Mode	SEVERE

*Vanguard rates security configuration errors as:

SEVERE (needs immediate remediation)
HIGH (needs plan of remediation for some point in the relatively near future)
MEDIUM (needs plan of remediation for some point in the future)
LOW (should be remediated when time and resources permits)

As of 7/22/15

z/OS Security Maturity Model



First step is establishing an IAM framework to properly provison and deprovision access to z/OS resources and enhance the productivity of the oragnization through Role Based Access models.

Productivity

IDENTITY & ACCESS MANAGEMENT

Second step is establishing a security operations monitoring framework that effectively monitors the z/OS environment for intrusions and misuse of resources.

Monitor

OPERATIONAL EXCELLENCE

Integrity

POLICY ENFORCEMENT

Third step is establishing a security policy for z/OS and ensuring the policy is enforced at all times to ensure the integrity of the z/OS platform.

Integration

RISK ANALYTICS

Fourth step is establishing and maintaining a data security warehouse where risk analysis is performed to determine unusual data usage patterns that may be an indication of a security breach or fraud.

Questions